Efficient XML Interchange (EXI) with XML Signature and Encryption: Reuse and Opportunity

Stephen D. Williams - sdw@lig.net / swilliams@hpti.com

Content:

• What is EXI?
• XML Signature and Encryption
  – EXI group position
  – SDW position
Efficient XML Interchange

- XML Infoset encoding
- Encoded for size and processing efficiency – broadly competitive (XML-PER)
- Binary blobs (a la b64), scalars, bit-oriented
- With or without schema-based factoring
- XML fragments for chunking or streaming
- Intended for current and much more broad market
  - Embedded and constrained devices
  - High speed transactions
Efficient XML Interchange

• Supports self-contained subtrees
  – An element that has no ties to surrounding document
  – Allows efficient copy
  – Ideal for signing and encryption
EXI Group Position

• Baseline option:
  – XML Signature and Encryption used as is – conversion to XML 1.1, C14N, etc.

• EXI inspired or tailored improvements:
  – EXI-efficient enveloping, C14N, self-containedness
  – Lightweight signing and encryption
    • Fewer features, less processing overhead
EXI Group Position (2)

- Schema-informed encoding
  - Schema information is used as shared knowledge to gain compactness
    - Information is “Externalized” from data instances
      - Structure
      - Typing
      - Identity / naming / namespaces
      - Values
  - Encoder and receiver need exact same schema
  - Familiar external references signature problem
SDW Position

• XML Meta Structure Instance (XMS)
  – Shared encoder grammar and table state
  – Something like a “compact schema”
    • Created from any kind of schema language, example, template, or other source
  – Encoded in EXI, sharable at runtime
  – Model: Send XMS, then instances encoded relative to it
  – Signature: Share signed XMS earlier or during transaction
SDW Position (2)

• Deltas
  – Parents with delta children instances
  – Changes from the parent
  – Alternate model for incremental document evolution with signing
  – High-level and low-level deltas are distinct ideas
  – Includes streaming models of XML fragments
SDW Position (3)

- EXI does what ASN.1: {BER/PER/DER/XER} do better in an XML-flavored fashion

- Should certificates and other PKCS standards become EXI encoded?
  - No: Deeply embedded, many libraries / certs
  - Yes: smaller code footprint, simpler APIs, faster evolution due to XML flexibility

- Can PKCS instances be made more efficient? Specialized for constrained environments?
Changes to consider

- Two part signatures: preamble, signature data
  - Enables streaming
- Lightweight signing and encryption
- EXI-optimized
  - Enveloping
  - Signature
  - C14N
- Parent / child
  - Schema / XMS
  - Fragments / Deltas